Ringe mit distributivem Faktorverband

Cohn, Paul M.

Veröffentlicht in:
Abhandlungen der Braunschweigischen
Wissenschaftlichen Gesellschaft Band 33, 1982,
S.35-40

Verlag Erich Goltze KG, Göttingen

Ringe mit distributivem Faktorverband

Von **Paul M. Cohn,** London

1. Dedekind hat zwei Arbeiten über Verbände geschrieben [5,6]; wenn man sie liest, sieht man wie gut wir es heute haben mit der graphischen Darstellung von Verbänden. Z.B. stellt er den kleinsten nichtmodularen Verband und den kleinsten modularen nichtdistributiven Verband durch Tabellen dar, während wir heute den ganzen Tatbestand bequem aus den folgenden Diagrammen entnehmen:

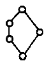


Abb. 1

Abb. 2

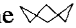
Dedekind's Arbeiten enthalten keinerlei Abbildungen; es ist erstaunlich, wie weit er trotzdem die Untersuchung trieb, indem er z.B. die freien distributiven und modularen Verbände mit 3 Erzeugenden (mit 18, bzw. 28 Elementen) bestimmte. Ich will hier nicht näher auf all seine Resultate eingehen, möchte aber doch seine Bezeichnungsweise kurz erwähnen, weil sie auf die ursprünglichen Anwendungen hinweist. Wir haben folgenden Diktionär:

Verband	Dualgruppe
modular	vom Modultypus
distributiv	vom Idealtypus.

Also Dedekind würde sagen, daß die ganzen Zahlen hinsichtlich der Teilbarkeit eine Dualgruppe vom Idealtypus bilden, während wir von einem distributiven Verband sprechen. Allgemeiner trifft dies zu für die Ideale eines Zahlkörpers, oder sogar in irgendeinem Dedekind-Ring (d.h. ZPI-Ring). Am einfachsten läßt sich das so einsehen: In einem Dedekind-Ring bilden die gebrochenen Ideale eine Verbandsgruppe, und jede Verbandsgruppe ist notwendig distributiv ([3], S. 294). Dagegen ist der Idealverband im Polynomring k[x,y] nicht distributiv, wohl aber der Verband der Hauptideale.

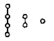
Bevor ich zu meinem eigentlichen Thema komme, will ich nur kurz folgende Frage stellen: Welche distributiven Verbände kommen hier vor? Um Unendlichkeitsfragen zu vermeiden, sehen wir uns den Verband aller Teiler einer festen Zahl m an, also den **Faktorverband** von m. Hier werden durchaus nicht alle distributiven Verbände verwirklicht, z.B.  kommt nicht vor. Um den Sachverhalt zu beschreiben, erinnern wir an folgende Dualität (Anti-Äquivalenz) von Kategorien. Es sei DL die Kategorie der endlichen distributiven Verbände (und Homomorphismen) und POS die Kategorie der endlichen teilweise geordneten Mengen. Dann ist $DL \cong POS^{op}$ vermittels der Abbildungen:

$P \mapsto P^*$ Verband der unteren Abschnitte,
$L \mapsto L^*$ Menge der vereinigungsirreduziblen Elemente.

(Vgl. [4], Kapitel 4). Z.B. der Verband  entspricht der Menge , und der freie distributive Verband (vgl. [8], S. 58) entspricht der Dreizack-Krone .

Nun läßt sich leicht zeigen

Satz 1 *([1], [4], S. 167) In jedem faktoriellen Ring sind die den Faktorverbänden entsprechenden Mengen gerade die Unionen von Ketten.*

Beispiel: $720 = 2^4 \cdot 3^2 \cdot 5$ 

Wir wenden uns jetzt dem nichtkommutativen Fall zu; hier zeigt sich, daß **alle** endlichen distributiven Verbände als Faktorverbände auftreten.

2. Wenn man allgemein einen kommutativen Integritätsbereich R betrachtet, so definiert die Teilbarkeit auf R eine vorgeordnete Menge. Sei U die Gruppe der Einheiten, dann ist R/U geordnet, und wir können fragen, wann R/U ein Verband ist. Das ist genau dann der Fall, wenn R ein HCF-Ring (= GGT-Ring) ist. Da dieser Verband automatisch in einer Verbandsgruppe liegt, ist er notwendig distributiv.

Wir sehen uns jetzt den nichtkommutativen Fall an; hier geht die Gruppeneigenschaft jedenfalls verloren. Nehmen wir $0 \neq c \in R$, so lassen sich die Linksteiler von c teilweise ordnen, und entsprechend die Rechtsteiler: Ist $c = a_1 b_1 = a_2 b_2$, dann ist

$$a_1 = a_2 d \Leftrightarrow b_2 = d b_1.$$

Hierauf beruht das Prinzip der faktoriellen Dualität ([4], S. 119):

$$L(cR,R) \cong L(Rc,R)^{op},$$

wo L(cR,R) den Verband der Rechtshauptideale zwischen cR und R bezeichnet, und entsprechend für L(Rc,R). Um einen Verband zu erhalten, muß man natürlich wieder die Existenz vom GGT voraussetzen, aber der Verband braucht dann noch nicht modular zu sein, geschweige denn distributiv. Die Modularität folgt, wenn L(cR,R) ein Teilverband des Verbands aller Rechtsideale ist, z. B. sobald die Summe je zweier Rechtshauptideale wieder Rechtshauptideal ist; laut Definition ist dies ein **Bezout-Bereich.** Diese Ringklasse läßt sich wesentlich erweitern, wenn man nur verlangt, daß die Summe von je zwei Rechtshauptidealen mit nichttrivialem Durchschnitt Rechtshauptideal ist; dies genügt ja, um die Modularität von L(cR,R) zu erzwingen. Die so definierten Ringe heißen **schwache Bezout-Bereiche** oder auch **2-Firs.**

Wir betrachten also jetzt 2-Firs, oder etwas spezieller Firs. Ein **Fir** (= Freiidealring) ist ein Ring R, in dem jedes (Rechts- oder Links-)Ideal frei als Modul über dem Ring ist, mit wohlbestimmtem Rang.

3. In einem kommutativen Ring sind zwei Elemente stets linear abhängig über dem Ring: $ab - ba = 0$. Daher ist ein kommutativer Fir einfach ein Hauptidealbereich, und selbst die nichtkommutativen Hauptidealbereiche sind noch Firs, aber das erschöpft diese Klasse bei weitem noch nicht. Insbesondere ist jede freie Algebra $k\langle X\rangle$ mit freiem Erzeugendensystem X über einem Körper k ein Fir, sowie das freie Produkt von Körpern $K \ast_k L$. All diese Ringe haben also modularen Faktorenverband und die Frage erhebt sich: Wann ist der Faktorenverband distributiv?

Man sieht leicht, daß ein Hauptidealbereich nur dann distributiven Faktorverband hat, wenn er invariant ist (d.h. alle Ideale sind zweiseitig, vgl. [4], S. 155). Nun hat man folgende interessanten Sätze von Bergman ([1], vgl. [4], S. 167):

Satz 2. Jede freie Algebra $k\langle X\rangle$ *hat distributiven Faktorverband.*

Genauer hat man

Satz 3. Jeder endliche distributive Verband kommt als Faktorverband in $k\langle X\rangle$ *(für genügend großes X) vor.*

Hier genügt es $|X|$ gleich der Breite des Verbandes zu nehmen. Z.B. der freie distributive Verband mit drei Erzeugenden entspricht dem Element in $k\langle x,y,z\rangle$:

$$(x^2+x)[(y(x^2+x)+1)z+1)](y(x^2+x)+1).$$

Etwas allgemeiner kann man für jeden Schiefkörper K mit zentralem Unterkörper k den freien Tensor K-Ring $K_k\langle X\rangle$ erklären als freien K-Ring mit Erzeugenden-System X und definierenden Relationen

$$\alpha x = x\alpha \quad \text{für } x \in X,\ \alpha \in k.$$

Dieser Ring ist stets ein Fir (vgl. [4], Kapitel 2), hat aber i.a. nicht distributiven Faktorverband. Und zwar läßt sich zeigen [2]:

Satz 4. Sei E/k eine kommutative echte Körpererweiterung.
(i) Wenn E/k eine Galoiserweiterung ist, so hat $E_k\langle X\rangle$ *nicht distributiven Faktorverband,*
(ii) wenn E/k rein inseparabel ist, so hat $E_k\langle X\rangle$ *distributiven Faktorverband.*

Wenn E/k separabel aber nicht Galois ist, oder wenn E nichtkommutativ ist, so ist die Antwort nicht bekannt.

Der Beweis von (i) benutzt eine Zerlegung von $E_k\langle X\rangle$ in ein freies Produkt von schiefen Polynomringen, während (ii) mit Hilfe der Bergman'schen Koproduktsätze bewiesen wird (vgl. [2]).

Um ein Beispiel für Satz 4 zu geben, benutzen wir folgenden

Hilfssatz. Ein 2-Fir hat distributiven Faktorverband genau dann, wenn keine Gleichung der Form

(1) $\quad ax - yaz = 1,$

mit einer Nichteinheit a gilt.

Der Beweis beruht darauf, daß die Gleichung (1) einem Diagramm wie in Abb. 2 entspricht ([4], S. 153, und auch [2]).

Sei jetzt $E = k(\alpha)$, wo $\alpha^2 = a \in k$, aber $\alpha \notin k$ (und Char. $k \neq 2$). Wir setzen $y = x - \alpha^{-1} x \alpha$, dann ist $\alpha y = -y\alpha$, also $(y+\alpha)\alpha + \alpha(y+\alpha) = 2a$, und hieraus leitet man leicht eine Gleichung (1) für die Nichteinheit $y+\alpha$ ab.

In Charakteristik $p \neq 0$ nehmen wir $E = k(\alpha)$, wo α Wurzel der Gleichung $x^p - x = a$ ist ($a \in k$), und α nicht in k liegt. Setzt man $y = \sum_0^{p-1} (\alpha+1)^{-i} x \alpha^i$, so gilt $\alpha y = y(\alpha+1)$, also hat man

$$(y+\alpha)(\alpha+1) - \alpha(y+\alpha) = \alpha,$$

woraus wieder eine Gleichung (1) folgt.

4. Ich will noch etwas über den Beweis von Satz 2 sagen, ohne auf alle Einzelheiten einzugehen. Der Satz ist durchaus nicht trivial; ich vermutete ihn etwa 1963, konnte ihn aber nicht beweisen. Ich fand aber andere Bedingungen für Distributivität, mit deren Hilfe es G.M. Bergman 1966 gelang, den Satz zu beweisen. Es ist zweckmäßig, eine zwischen den Firs und 2-Firs stehende Klasse zu betrachten, die **Semifirs.** Sie sind definiert als Ringe, in denen jedes endlich erzeugte (Rechts- oder Links-) Ideal frei ist, von eindeutig bestimmtem Rang.

Wir brauchen noch einige weitere Definitionen. Es sei A eine beliebige Matrix über einem Ring R, dann wird der **innere Rang** $\varrho(A)$ von A definiert als die kleinste Zahl r derart, daß sich A als PQ schreiben läßt, wo P eine Matrix mit r Spalten ist. Insbesondere, wenn A quadratisch, etwa $n \times n$ ist, und $\varrho(A) = n$, so wird A **voll** genannt. Wenn eine Matrix A aus R in einem R enthaltenden Körper invertiert werden kann, so muß A in R voll sein; umgekehrt hat ein Semifir stets einen Quotientenkörper U, in dem jede volle Matrix invertiert werden kann. U ist eindeutig bestimmt (bis auf Isomorphie) und wird **universeller Quotientenkörper** für R genannt.

Ein Semifir R heißt **konservativ**, wenn R k-Algebra ist, und (i) R und $R \otimes_k k(t)$ Semifirs sind, und (ii) jede volle Matrix von R[t] über $R \otimes k(t)$ voll bleibt. Es ist nicht schwer zu zeigen, daß $k\langle X\rangle$ konservativ ist, und Bergman konnte zeigen, daß jeder konservative Semifir distributiven Faktorverband hat.

Nun führten kürzlich Dicks und Sontag [7] eine Verallgemeinerung des Semifir-Begriffs ein, welcher eine unerwartete Rolle für den Bergmanschen Satz 2 spielt. Sie betrachteten Ringe mit der Eigenschaft, daß ein sie enthaltender Körper existiert, in dem jede volle Matrix invertiert werden kann. Diese Ringe wurden **Sylvester-Ringe** genannt, weil sie auch durch das Gelten des Sylvesterschen Nullitätsgesetzes:

$$\varrho(AB) \geqq \varrho(A) + \varrho(B) - n, \quad \text{wo } A \in {}^rR^n,\ B \in {}^nR^s$$

gekennzeichnet werden. Offenbar ist jeder Semifir ein Sylvester-Ring (nach dem vorher gesagten), weiterhin, wenn P Hauptidealbereich ist, so ist $P\langle X\rangle$ Sylvester-Ring, z.B. $k[t]\langle X\rangle = k\langle X\rangle[t]$. Jetzt hat man folgende Verallgemeinerung von Satz 2 (vgl. [2]).

Satz 5. Es sei R ein Semifir, dann folgt aus jeder der unten genannten Eigenschaften die nächste:
(a) R ist ein konservativer Semifir,
(b) R[t] ist ein Sylvester-Ring,
(c) R ist ein Semifir mit distributivem Faktorverband.

Beweisskizze. a ⇒ b. $R\otimes k(t)$ ist ein Semifir, hat daher einen universellen Quotientenkörper U. Jede volle Matrix von R[t] ist nach Voraussetzung voll über $R\otimes k(t)$, also invertierbar über U, daher ist R[t] ein Sylvester-Ring.

b ⇒ c. Wir setzen (b) voraus und betrachten eine Gleichung der Form (1) (im Hilfssatz): $ax-yaz=1$. In R[t] hat man

(2) $$a(tz+x)-(t+y)az=1.$$

Nun ist ein Sylvester-Ring projektiv-frei [7], d.h. jeder projektive Modul ist frei, also lassen sich die Zeile $(a, t+y)$ und die Spalte $\binom{tz+x}{-az}$ zu gegenseitig inversen Matrizen ergänzen:

$$A=\begin{pmatrix} a & t+y \\ p & g \end{pmatrix},\quad A^{-1}=\begin{pmatrix} tz+x & -f \\ -az & q \end{pmatrix},\ \text{wo } f,g,p,q\in R[t].$$

Es gilt $aza=qp$, also haben p, q Grad 0 in t. Weiterhin ist

(3) $$af=(t+y)q,\quad p(tz+x)=gaz.$$

Ein Gradvergleich zeigt, daß f,g linear in t sind. Wir setzen

$$f=f_1t+f_0,\quad g=g_1t+g_0,\quad f_i,g_i\in R,$$

dann führt (3) auf $af_1=q$, $p=g_1a$, also

$$\begin{pmatrix} a & t+y \\ p & g \end{pmatrix}=\begin{pmatrix} 1 & t+y \\ g_1 & g \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}.$$

Somit ist a Einheit, und (c) ist bewiesen.

Keine von den beiden Implikationen läßt sich umkehren. Wenn (b) gilt, braucht $R\otimes k(t)$ kein Semifir zu sein (man nehme $R=E\langle X\rangle$, wo E nicht algebraisch über k ist). Für b ⇒ c brauchten wir nur die Tatsache, daß R Semifir und R[t] 2-projektiv-frei ist, also ist eine Umkehrung nicht zu erwarten.

Literaturverzeichnis

[1] G.M. Bergman, Commuting elements in free algebras and related topics in ring theory (Thesis, Harvard University 1967).
[2] G.M. Bergman and P.M. Cohn, to appear.
[3] G. Birkhoff, Lattice theory, 3rd ed., Amer. Math. Soc. (Providence 1967).
[4] P.M. Cohn, Free rings and their relations, LMS monographs No. 2, Academic Press (London, New York 1971).

[5] R. Dedekind, Über Zerlegungen von Zahlen durch ihre größten gemeinsamen Teiler, Festschrift techn. Hochschule Braunschweig, 69. Vers. Deutscher Naturforscher u. Ärzte (1897) 1–40, No. XXVIII, Ges. Werke, II, 103–147.
[6] R. Dedekind, Über die von drei Moduln erzeugte Dualgruppe, Math. Ann. 53 (1900) 371–403. No. XXX, Ges. Werke, II, 236–271.
[7] W. Dicks and E.D. Sontag, Sylvester domains, J. pure and applied Algebra 13 (1978) 243–275.
[8] G. Grätzer, General lattice theory, Birkhäuser Verlag (Basel 1978).